CLAIMS

What is claimed as new and desired to be protected by Letters Patent of the United States is:

1. An internet service provider (ISP) VPN network comprising:

a plurality of edge routers;

a plurality of core routers adapted to allow communication between said plurality of edge routers;

a VPN application in communication with a first one of said plurality of edge routers, said VPN application having a first IP address; and

a black-hole router in communication with said core routers, said black-hole router adapted to inject a second IP address into said ISP VPN network, said second IP address comprising:

the same address as the first IP address;

a higher preference value than said first IP address; and

a community value such that when said second IP address is injected, a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said first IP address to said black hole router.

2. The ISP network of claim 1, wherein said ISP system is a Multiprotocol Label Switching Virtual Private Network (MLS VPN) ISP.

3. The ISP network of claim 1, wherein said black-hole router injects said second IP address in response to a Distributed Denial of Service (DDoS) attack on said VPN application.

4. The ISP network of claim 1, wherein said community value can be changed in real-time by said black-hole router.

5. The ISP network of claim 1, wherein said ISP network utilizes dynamic routing protocols in combination with community-based route filtering to propagate the injected second IP address to said edge routers.

6. The ISP network of claim 1 wherein when said second number of edge routers directs VPN traffic, addressed for said first IP address, to said black hole router, said black hole router is adapted to receive such traffic as black-holed-traffic, said black-hole router adapted to analyze said black-holed traffic in order to determine a ratio of attack traffic to legitimate traffic.

7. The ISP network of claim 1, further comprising at least one route reflector, each one of said route reflectors being connected to a different set of edge routers from said plurality of edge routers, said route reflectors being adapted to update said edge routers with route instructions, such route instructions including said injected second address.

8. An ISP network comprising:

a plurality of edge routers;

an application in direct or indirect electrical communication with a first one of said plurality of edge routers;

said application having a first IP address such that VPN traffic addressed for said first IP address and entering said ISP network at any one of said plurality of edge routers, is routed to said application;

a black-hole router;

a router adapted to inject an instruction into said ISP network, such that select edge router(s) redirect VPN traffic, which is addressed to said first IP address, to said black-hole router.

9. The ISP network of claim 8, wherein said injected instruction comprises a routing instruction having the same IP address as said first IP address, but with a higher preference than said first IP address and having a community value.

10. The ISP network of claim 8, wherein said ISP network is a MLS VPN ISP network.

11. The ISP network of claim 8, wherein said router and said black-hole router are the same device.

12. The ISP network of claim 8, wherein said injected instruction is a Border Gateway Protocol (BGP) routing instruction.

13. The ISP network of claim 8, wherein said black-hole router is adapted to receive redirected traffic from said select edge router(s) and to determine a ratio of attack VPN traffic to legitimate VPN traffic found in said redirected traffic.

14. The ISP network of claim 8, wherein said router injects said instruction when said application is experiencing a DDoS attack.

15. A method of managing a DDoS attack on an application within an ISP, said application having a first IP address, said method comprising:

injecting a BGP routing instruction into said ISP when said DDoS attack is occurring;

redirecting, at selected edge routers, VPN traffic addressed for said first IP address to a black-hole router;

directing, at other edge routers, VPN traffic addressed for said first IP address to said application that is experiencing said DDoS attack.

16. The method of claim 15, wherein said ISP network is a MPLS VPN ISP network.

17. The method of claim 15, further comprising:

receiving, at said black-hole router, said redirected VPN traffic; and

determining an amount of attack traffic therein.

18. The method of claim 15, further comprising changing, in real-time one or more of the selected redirecting edge routers to a directing edge router.

19 The method of claim 15, wherein injecting said BGP routing instruction into said ISP is done by providing said BGP routing instruction to a route-reflector for disseminating said BGP routing instruction to other route reflectors within said ISP network.